AFRL-IF-RS-TR-2004-68
Final Technical Report
March 2004

LIGHTWEIGHT CRYPTOGRAPHIC TECHNIQUES

Northwestern University

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. K251

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2004-68 has been reviewed and is approved for publication.

APPROVED: /s/

ROBERT L. KAMINSKI
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, JR., Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	MARCH 2004	Final Jun 02 – Jun 03

4. TITLE AND SUBTITLE
LIGHTWEIGHT CRYPTOGRAPHIC TECHNIQUES

5. FUNDING NUMBERS
C - F30602-00-2-0536
PE - 62302E
PR - K251
TA - 25
WU - A1

6. AUTHOR(S)
Horace P. Yuen, Majjid Sarrafzadeh,
Agnes Chan, and Aggelos Katsagelos

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Northwestern University
Evanston Illinois 60208-3113

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington Virginia 22203-1714

AFRL/IFG
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2004-68

11. SUPPLEMENTARY NOTES
AFRL Project Engineer: Robert L. Kaminski/IFG/(315) 330-1865/ Robert.Kaminski@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***
The objective of this project was to develop new cryptographic techniques, and to modify the important existing ones, for applications to encryption and authentication in energy-constrained sensors with limited memory and computational capability. The goal was to minimize power consumption in order to maximize the lifetime of the sensor operation and the amount of useful processing that can be carried out within the lifetime. For handling low power stream cipher on small handheld devices, Software Based Stream Ciphers were implemented and compared with other software based encryption algorithms. A new spread signal cryptographic technique has been developed that promises significant additional security with no new bandwidth or power overhead. New design methodologies have been developed for power conscious systems with power/security tradeoffs. The impact of imaging sensors on benchmark and operational scenarios related to target tracking in a wireless sensor network has been investigated in an added task. Leveraging on the state-of-the-art in image-based tracking, new algorithms and novel methods have been discovered that enhance the capability of existing imaging technologies.

14. SUBJECT TERMS
Sensor Network, Cryptography, Network Security, Video Communications

15. NUMBER OF PAGES
26

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

TABLE OF CONTENTS

List of Figures

List of Tables

I. Introduction

Various microsensor networks such as those exemplified by Bluetooth technology have emerged, with further miniaturization toward the nanoscale by utilizing commercial smartcard technology, for military and other applications. The problem of information security is of central importance in both of these types of short-range wireless radio networks, which share the common characteristics of limited resources for communication and computation. The individual sensors need to be able to authenticate one another and to communicate securely at Mbps rate up to 100 m distance, and perhaps occasionally with a larger base station, in order to perform certain joint signal processing and monitoring operations, to hold some data in memory, and to deliver them to their final destination. One overall goal would be to minimize the power consumption in order to maximize the lifetime of the sensor network operation and the amount of useful processing. Power minimization has been an important consideration in computation for some time. The Crusoe processor supposedly saves power by having more functions implemented in software, and reversible logic may hold some promise in the future for special hardware power reduction. Such general future possibilities, while useful, are not specifically tuned to the problem of security.

The objective of this project is to develop cryptographic techniques that achieve a high level of performance in terms of both security level and encryption/decryption rates while at the same time offering a new level of power efficiency for energy-constrained sensors. They would be useful with any hardware, including the Crusoe processor and reversible logic when available. Many cryptographic techniques have been developed in the similar context of cellular phones, Bluetooth, and smartcard applications. Some considerations of power efficiency are given in the first two of these technologies, which, however, only involve linear feedback shift register and the new block cipher SAFER$_+$ whose security levels are not very high [Sch96], [MOV97]. Energy has not been an issue in smart cards, which are powered mainly by machine terminals. An important consideration in our project is to integrate the forward error control necessary for reliable communication to the cryptographic mechanisms, which are often compromised by communication coding -- a good example of such a compromise is found in the cellular IS-95 CDMA protocol. We have developed entirely new signal/noise cryptographic techniques as well as new stream cipher algorithms to solve this problem. We have also applied various standard and novel VLSI power minimization techniques to modify various cryptoalgorithms which are compared in an easy-to-use form.

There are three major functions in a cryptographic system: key management, authentication and encryption. The algorithms we choose to study and develop include the standard ones based on shared secret key, dual public/private keys, ones for random number generations, for stream ciphers, and new ones based on communication signaling. They can be used as modules in a variety of encryption/decryption, key distribution, message authentication, and identification (user authentication) protocols. It is not our purpose to investigate and develop such protocols, although they would also have effect on power assumption, except to note the following. In many applications of sensor networks, there is no need to have separate keys for different cells or groups for many

cryptographic functions, such as encryption from one point to a distant point. Use of the same key would greatly reduce the power consumed by decryption/re-encryption when hopping from one cell to another. On the other hand, the frequent change of session keys, while power consuming, enhances the security level and could lead to a final saving of total power if an otherwise less secure but also less power consuming algorithm can be used instead.

The project consists of three major, inter-related tasks and one additional task

- Task A: Novel Stream Ciphers
- Task B: New Spread Signal Cryptography
- Task C: Power Prediction and Reduction
- Task D: Image and Video Processing and Communications.

II. TASK A: Novel Stream Ciphers

Introduction

In this project, we address the problem of designing and implementing efficient cryptographic protocols and algorithms for low power devices. The goal is to ensure that user authentication, communication security and key management problems can be handled efficiently over low power devices. To this end, we consider

1. the design and implementation of Software Based Stream Cipher (SSC2) on small handheld devices, such as Palm Pilots and iPaqs.
2. performance comparison of SSC2 with other software based encryption algorithms.
3. implementation of Mutually Authenticated Key Exchange Protocol using SSC2 for data integrity and privacy.
4. the implementation of a group key management system to manage dynamic changes of membership within a group.

Software Based Stream Cipher

Chan and Zhang [1] first proposed the design of Software Based Stream Cipher, SSC2, in 2000. To ensure computational efficiency in software, we design the cipher based on a byte-based (or word-based) linear feedback shift register, together with simple nonlinear functions such as modulo add, carry and shifts. Figure 1 provides a schematic design of the stream cipher. The security of the cipher against currently known attacks has been analyzed and published in [1,2]. Other cryptographers [3] have also studied the vulnerability of the cipher.

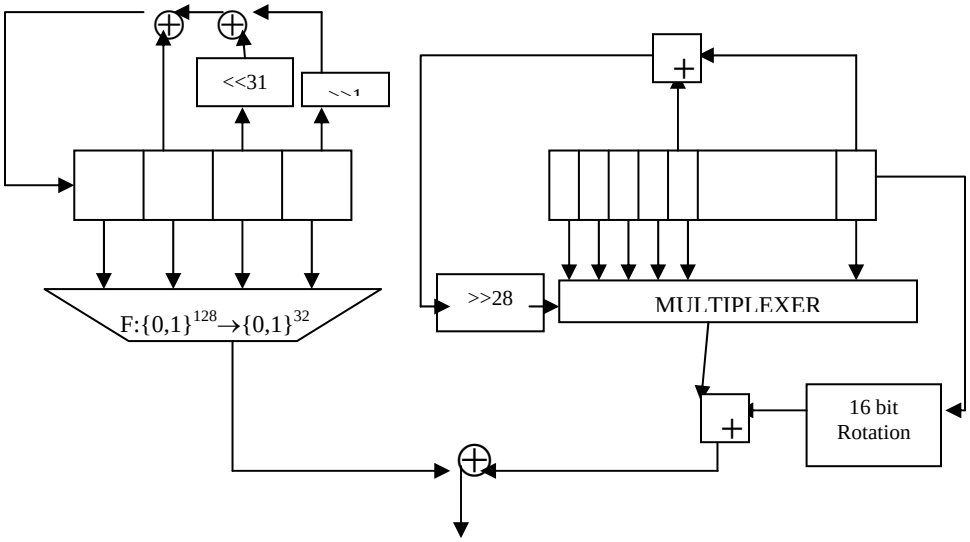

Figure 1: Schematic Design of SSC2

The performance of the cipher on low power devices, such as Palm OS, was compared with other software based ciphers (given in Table 2), in particular, the Alleged RC4 and Software Encryption Algorithm (SEAL). It is observed that SSC2 outperforms both algorithms. The results are documented in [4] attached in Appendix A.

Table 1 Performance Comparison of Software Based Encryption System over Palm OS (Throughput in Bytes per second)

Data size / Algorithm	2 KB	50 KB	4 MB
SSC2	32,604	35,804	35,501
ARC4	30,768	32,100	31,699
SEAL	2,469	28,723	51,396

Mutually Authenticated Key Exchange and Key Management

Since SSC2 is a symmetric key cipher, the efficiency of key management has to be considered. We first consider client-server model where the client is low powered and requires lightweight cryptographic algorithms, the server may be a base station with battery and computational power equivalent of a desktop. We implemented a mutually authenticated key exchange protocol where low power clients depend on symmetric key operations based on SSC2 and the servers depend on public key cryptographic operations. Table 3 below shows the performance comparison of the Server Specific Mutually Authenticated Protocol (SSMAKEP) and the Station to Station (STS) Protocol used over the wired network.

Table 2 Performance Comparison of SSMAKEP and STS Protocol (authentication completed in msec)

	SSMAKEP	STS
Palm OS vs. Linux	220 – 260 msec	738,740 msec
Linux vs. Linux	17 – 27 msec	494 – 515 msec

Once the client and server shares a common key between them through the key exchange protocol, clients with small devices will then communicate through a common group key provided by the server. Since the group membership changes dynamically, the server has to provide a key update service that clients can receive the new group key efficiently and securely. A Group Key Management Scheme has been implemented as part of the effort in the project.

III. TASK B: New Spread Signal Cryptography

We have invented a new technique that utilizes proper signal modulation and channel noise but without these weaknesses, and also without bandwidth expansion. The idea is based on analogy with quantum cryptography [BBA92] and can be considered a generalized form of spread spectrum -- "spread signal" (SSi) in the given signal space for which the important general variable is signal location in the space, parameterized by its amplitude and phase in addition to frequency. The idea can be applied to any digital modulation format including the usual phase-shift keying (PSK) and frequency-shift keying (FSK) convenient for wireless applications, as well as amplitude-shift keying (ASK) that allows incoherent detection without bandwidth consumption. For definiteness we introduce it in the context of M-ary phase-shift keying (MPSK) modulation in which one of M possible signals of energy E lying on a circle of a two-dimensional signal space, typically from the two quadratures of a single-frequency signal, can be transmitted as indicated in Fig. 2. The actual signaling scheme to be employed is, say, a binary phase-shift keying (BPSK) system with M/2, for even M, possible pairs of opposite signals on the circle selected out of the M PSK signals. As depicted in Fig. 3a, if the receiver needs only to discriminate between a BPSK pair, say in additive white Gaussian noise (AWGN), the optimal decision can be arranged as usual for equiprobable inputs, with decision region I for value I and region II for value 0. For any signal-to-noise $SNR_B = 2E_0/N_0$, one obtains

$$P_e \sim \exp\{-SNR\} \qquad (1)$$

However, if the receiver has to discriminate a large number of M PSK signals in noise level N_1 with signal energy E_1 the same error behavior (1) is obtained with a signal-to-noise ratio $SNR_M = (4\pi^2/M^2) \times E_1/N_1$ for large $M \geq 10$ as seen in Fig. 3b. A small noise N that would not cause an error in BPSK may, by pushing the signal for 1 outside its decision region (a) to the decision region (b) for a 0. Thus,

$$SNR_M / SNR_B = (2\pi^2/M^2) \times (E_1N_0/E_0N_1) \qquad (2)$$

and the receiver performance can be made to be much poorer than the BPSK case by making M sufficiently large for any N_0, N_1,E_0, E_1. Now the transmitter modulates a data bit stream by selecting one of the M/2 BPSK pairs for each bit according to some fixed rule shared by the receiver but unknown to the eavesdropper who, not knowing which pair to use, would not be able to identify the signal in a way similar to PN spread spectrum. In an AWGN channel or a coded communication system where multipath, fading, and interference are important, the error probability P_e can be made exponentially small in the SNR as in (1). From (2), just a modest M~40, for $N_0 = N_1$ and $E_0 = E_1$, would bring the eavesdropper's SNR 20 dB down to an undetectable level. There is a lot of flexibility in picking the secret rule for BPSK pair selection, with different levels of efficiencies and security. A keyed LFSR with variable seed length and connection polynomial should be adequate for most purpose, because the ciphertext of the LFSR is not available to an eavesdropper from the MPSK modulation and channel noise addition which provides an automatic probabilistic encryption without any additional resource.

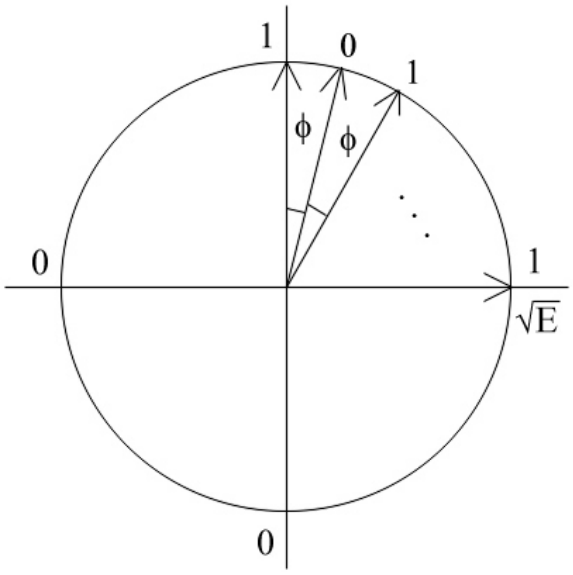

Figure 2: M-ary phase shift keying signals with M/2 different binary PSK pairs

It is important to note that the noise N_1 the attacker has to suffer need not be greater than N_0, nor the signal energy E_1 need be smaller than E_0. Indeed, for any signal-to-noise advantage on one BPSK pair the attacker may have, it can be overcome by a sufficiently large M from (2). Typically, the attacker has to suffer some channel noise, at least the noise in his detectors. His signal level also cannot go higher than what is transmitted by the sensor.

The advantages of this scheme include the following. First of all, it has no bandwidth expansion and can be used in conjunction with the usual spread spectrum technique useful for antijam purpose. Secondly, it is much more truly a probabilistic encryption compared to DS spreading in which each chip has only two levels, here it has M. Thus, the above-mentioned weaknesses in PN DS spreading are ameliorated. In particular, in contrast with CDMA IS-95, the communication code structure would not reveal useful information on the LFSR output sequence. Furthermore, in addition to having high security level and encryption rate at the signal modulation rate, it is also quite efficient in power consumption comparable to or better than a stream cipher, as very simple LFSR can be used. The disadvantages are that M-ary modulation is required compared to binary, that the eavesdropper's possible signal-to-noise level needs to be estimated so that a sufficiently large M in (2) is to be used, and that the technique is new and has not been extensively analyzed. In particular, careful cryptanalysis is needed to fully quantify its security level. In this project we propose to perform such studies using information theoretic and probabilistic techniques, with special emphasis on the utilities of this approach in lightweight encryption. We believe it is quite possible that the technique can be proved secure against every kind of known plaintext attack.

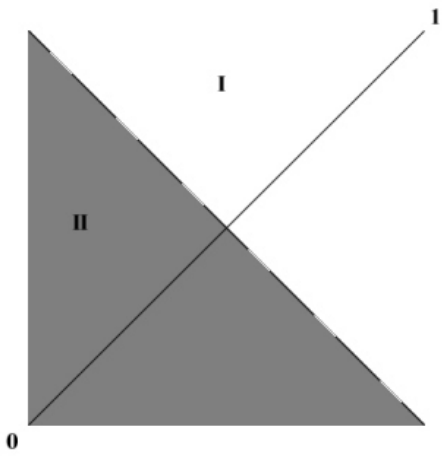

Figure 3a: Decision regions for BPSK

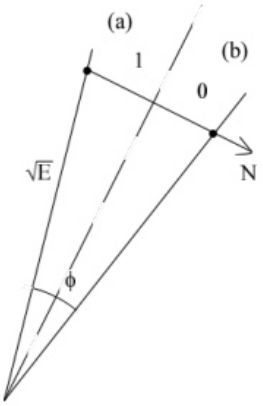

Figure 3b: Noise vector N interfering with neighboring BPSK

We have introduced another novel technique that significantly lessens the level of noise that is requires to be present in the above description. In this approach, the signal being transmitted is further randomized by an angle $\Delta\sigma$ so that the total error $\Delta\Phi + \Delta\sigma \leq \Pi$. The receiver does not need to know $\Delta\sigma$, and the technique is to be called deliberate signal randomization (DSR). With this technique we would sum the system as indicated in Fig. 4 where ENC represents a lower power encryption mechanism such as that of Task A. The seed key K determines a running key K' through ENC that executes the modulation first via Fig. 1 and then further randomized by DSR. As a consequence known plaintext attack on the key would involve an added search that is compounded on that ENC alone, and appears to be experimental in nature. The use of this technique has now been proposed for quantum cryptography in ref [5].

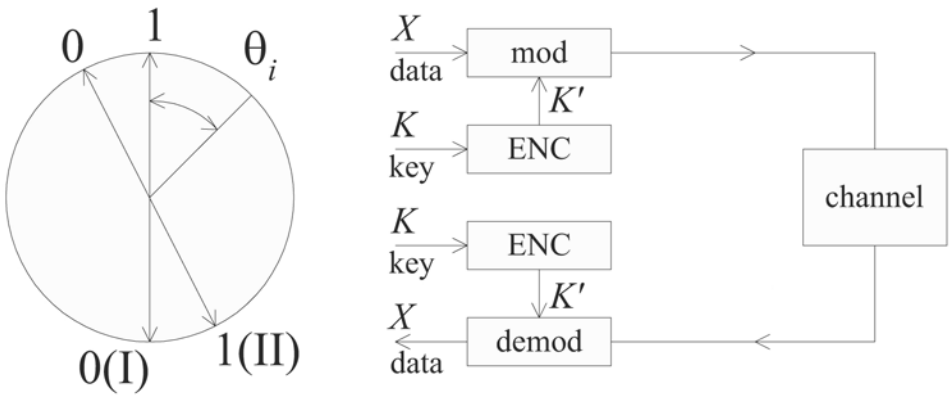

Figure 4: Combined SSi and Low-power encryption

IV. TASK C: Power Efficient Algorithms

The research effort has been focused in two directions. The first is directed towards the development of effective design methodologies and new design paradigms for power conscious systems. The second is looking into the architectural and implementation issues for generating power/security tradeoffs in cryptosystems. Both systems are 100% completed.

Design Methodologies and Paradigms for Power Aware Systems

We have developed methodologies for power optimization at gate level through dual voltages. In this work, we propose a provably good algorithm for voltage scaling in gate level circuits. Methodologies for simultaneous voltage scaling and gate sizing for power optimization have also been developed. These algorithms when combined with our novel delay budgeting procedure can result in large decrease in power dissipation at negligible performance penalty. At system level, we have developed an optimal power aware node-scheduling algorithm for wireless distributed sensor networks. It assists in optimizing power dissipation and improving system energy/lifetime.

The most important contribution in the last few months has been the development of the philosophy of predictability applied to power optimization and estimation. Power estimation is extremely hard because of the different and complex parameters involved. Predictability in such a scenario is key. Our latest research shows that the accuracy in prediction is strongly related to the design structure and more specifically resource binding. We have proposed cost functions that capture the notion of predictability in power at the resource binding stage. Two algorithms have been developed to address the predictability optimization problem. The first algorithm modifies the traditional network flow based methodology used for power driven resource binding and optimizes the predictability. The second algorithm is based on the left edge algorithm and treats the input scheduled data flow graph as an interval graph. A complete system has been developed that takes functions written in C as input and schedules the extracted DFGs in the required clock steps. This scheduled DFG is then subjected to resource binding using the algorithms mentioned above. Experiments on Media-Bench benchmark suite show that our methodologies lead to an average improvement of 81% in power predictability with around 13% power penalty in RTL designs. Some of the benchmarking C files used by us were extracted from crypto applications. This increase in predictability could be used to make better system decisions and optimizations.

Power Efficient Architectures for Crypto-Algorithms

We concentrated on the development of power efficient implementations for crypto-algorithms. We used the Synopsys design flow for experimental purposes. We have implemented initial versions of all basic blocks in the reduced –rank filter using VHDL. However the digital signal processing character of the design raises a number of hardware related design issues. The synthesizability of the design is also a major concern since the current synthesis tools constrain the specification language. This requires

detailed analysis; proper adjustment in the design and utilization of specific techniques to overcome these difficulties. Our main goal was to design architectures that enable efficient tradeoff between power dissipation and security. We have integrated these architectures and implementations with novel power aware design methodologies and paradigms for synthesizing highly power optimized implementations. The overall results are given in ref [6] – [25].

V. TASK D: Image and Video Processing and Communications

Introduction

The main objective of this project was to investigate the impact of video and imaging sensors on benchmark and operational scenarios related to target tracking in a wireless sensor network. This research was motivated by the observation that imaging sensors can offer useful and substantially different information on a target, which cannot be obtained by other sensing modalities that have been considered in the SensIT program, such as acoustic, seismic, and thermal. Leveraging on the state of the art in image-based tracking, the work was directed towards improving currently existing algorithms as well as discovering novel methods that would enhance the capabilities of existing imaging technologies. An overview of the end-to-end imaging-sensor-based tracking system envisioned in this research, and a discussion of the accomplishments and discoveries made during the project, are provided below.

Overview

The basic scenario that we considered was that of detecting a target as it enters a sensor field composed of wireless imaging sensors, and continuously tracking the 3-D position and velocity of the target as it moves through the field. We assumed that the imaging sensors have been arbitrarily positioned in the sensor field, and that they have arbitrary orientations.

In order to be able to accurately estimate the 3-D position of the targets, it is first necessary to calibrate the imaging sensors. We considered two types of calibration techniques, those that require a calibration grid, and self-calibration techniques that rely on scene features for calibration. The latter are preferable, as they do not depend on an object of known dimensions and position on the scene. Self-calibration techniques require the detection of correspondences between points in snapshots obtained from each camera. This is particularly difficult when the cameras are in a wide baseline configuration, which is typical when an arbitrary sensor placement is assumed. The problem is considerably easier in a narrow-baseline configuration when the cameras axes are assumed to be parallel. Thus, a significant portion of the project was devoted to the problem of robust feature point matching and camera calibration for the wide baseline case.

Another important problem in tracking using imaging sensors is the detection of moving targets. It is generally accepted in the computer vision community that this can be accomplished efficiently using background subtraction techniques. We implemented state-of-the-art subtraction techniques, and considered refinements that increase their robustness and accuracy.

An important consideration in the context of the SensIT program is that the imaging sensors are typically part of a wireless network, and thus, are constrained in their energy usage. Since imaging sensors in general consume more power than other less complex sensors, it is important to consider tracking algorithms that optimally select the set of

imaging sensors to be used for tracking, while the remaining sensors remain in an inactive, low power state. In this context, we developed a novel algorithm that selects an optimal set of imaging sensors in a scalable and distributed manner.

The main goal of the techniques we have studied for detecting and tracking targets is to minimize the amount of information that is transmitted between the wireless sensors, in order to conserve energy, and also, to minimize the probability of interception. In some critical cases, however, it may be necessary to transmit the raw video data. For such cases, we developed techniques that make efficient use of transmitter energy in video streaming over wireless channels.

The basic components of the system that were studied and developed during this project can be summarized as follows:

1. Wide-baseline camera calibration
2. Background subtraction for target detection
3. Optimal sensor selection for multiple sensor tracking
4. Low-transmission-energy techniques for wireless video communication

We now discuss the techniques in more detail.

Wide Baseline Camera Calibration

As we saw above, camera calibration is necessary for accurate estimation of target position and tracking. Camera calibration consists of estimating the camera position and orientation (extrinsic parameters) and the focal length, skew, aspect ratio, and principal point of the camera (intrinsic parameters).

There are two major approaches to calibration: **grid-based calibration**, which introduces a "foreign" object of known dimensions into the scene, and **self-calibration** which relies on constraints (epipolar, absolute conic) contained in the images themselves to obtain the unknown camera parameters. During the early stages of the project, we explored grid-based calibration techniques. A working system that uses planar circular control points was developed, and was able to calibrate cameras with high accuracy. However, in a realistic sensor network scenario, self-calibration techniques are obviously preferable. Using such techniques, cameras can be calibrated up to a scale factor. Complete Euclidian calibration can be achieved using some metric information about the scene, e.g., using GPS to obtain the baseline distance between cameras.

The main idea is to calibrate two or more cameras using snapshots of a moving target. The target motion provides several constraints on the camera parameters. When using two cameras, it can be shown that two target snapshots with 8 point correspondences per snapshot are necessary to calibrate the two cameras using a simplified camera model, which assumes that the aspect ratio of the camera pixels is known and that there is no skew. Such assumptions are reasonable for the current generation of cameras. Furthermore, the location of the principal point can be safely assumed to be at the center of the image plane, as it is known that small deviations in the location of the principal

point do not significantly affect the reconstruction accuracy. More importantly, if all of the intrinsic parameters except the focal lengths are available, then the calibration can be performed using only one snapshot from the two cameras. This assumption, which in many cases is quite realistic, simplifies the problem considerably and makes the solution more robust.

Self-calibration is performed by exploiting the epipolar constraint between images and calculating the fundamental matrix, which describes pixel correspondences between camera snapshots. Intrinsic parameters are obtained from fundamental matrices using the Kruppa equations, and extrinsic parameters are obtained by decomposing an essential matrix into its rotational and translational components.

The wide-baseline camera calibration problem was tackled in two major steps. First, we developed an improved feature point detection and correspondence algorithm that can be used to obtain an adequate number of accurate point matches for camera calibration. Second, since the point-matching algorithm also produces a large proportion of outliers (incorrectly matched points), we designed a robust camera calibration algorithm that can eliminate the outliers and accurately measure the camera parameters.

1. Feature Point Detection and Correspondence

We used an improved version of the Harris corner detector, which is commonly used to detect feature points. The Harris corner detector detects points in the image around which the image intensity varies significantly in two directions. Such points usually occur at corners of objects in the image, and can be consistently detected (using a Harris detector) in images of the object taken from varying viewpoints. We used a multiscale version of the Harris detector in order to detect feature points across multiple scales. We proposed an enhanced version of the multiscale Harris detector that exploits a scalespace filtering technique to further improve the feature point localization. The proposed enhancement selects points with high corner strength at larger scales and tracks them down through scalespace to smaller scales. This provides more accurate feature point localization, which is critical for camera calibration.

While images taken from cameras in a wide baseline configuration are generally related by a perspective transformation, it was assumed that within a small locally planar region the perspective transformation can be approximated by an affine transformation. Thus, once the feature points are detected, the image neighborhood around each feature is transformed into an affine invariant form using the concept of affine Gaussian scalespace. The affine invariant form of each point neighborhood is represented by a 15-element vector, which can then be used to match with vectors obtained from feature points in the image from another camera. The matching can be done using a Mahalanobis distance measure. The corresponding feature points in the two camera images are then those that have the closest affine feature vectors.

2. Robust Camera Calibration

We implemented a robust camera self-calibration algorithm and tested it on indoor and outdoor scenes using both manually and automatically selected feature points. The results were very good, demonstrating the efficacy of the approach. It was also found, however, that the process of fundamental matrix estimation is very sensitive to noise, especially when it results in feature correspondence mismatches, which in turn can cause the estimation to totally collapse. We implemented a Random Sample and Consensus Algorithm (RANSAC) in order to eliminate outliers caused by the feature detection algorithm, and also, to add robustness to the fundamental matrix estimation. The RANSAC tries different sets of feature points, chosen randomly, in order to find the best fit (that is, the one with the most inliers). Since the estimation requires at least seven point-correspondences, in order for RANSAC to work, it is necessary that the set of feature points contains at least seven correct correspondences. Once the outliers are detected and eliminated, then the correct epipolar lines can be obtained. To add further robustness and precision to the fundamental matrix estimation, the epipolar constraint gained from the initial fundamental matrix estimation can be utilized to obtain additional feature point matches in a second stage of the algorithm. To accomplish this, we utilized the epipolar constraint by searching for a matching feature point in the other image only in the neighborhood of the corresponding epipolar lines.

We also conducted further testing in order to evaluate the robustness of the algorithm under non-ideal conditions. Our tests demonstrate that the algorithm is able to perform well even at high noise levels (Gaussian, PSNR = 20dB) and on compressed images down to less that one bit per pixel (JPEG-standard compression), with a smooth degradation as the noise and compression increase. Such analysis is essential in evaluating the performance of the calibration algorithm, and as far as we know, has not been previously reported in the computer vision literature.

Background Subtraction

The following key considerations were taken into account in the design of the background subtraction algorithm:

1. **Adaptability to gradual changes in illumination:** As the time of day changes, the lighting conditions of the system also change. Therefore, the background model must be updated temporally based on the current lighting conditions in the scene.

2. **Robustness to vacillations in background:** In outdoor scenes, trees waving in the wind can cause a particular pixel in the image frame to be a projection of a part of a leaf (green), a branch of the tree (brown), or the sky (blue). In all these cases, the particular pixel should be labeled as background although its intensity may differ significantly between successive frames.

3. **Small training period:** Due to energy considerations in a wireless sensor network, the imaging sensor cannot be expected to remain active at all times. Therefore, the background subtraction algorithm must be able to initialize and generate a background model within a few seconds.

We used a simple, currently existing, background subtraction technique to obtain an initial segmentation of the background region. This technique is based on maintaining a non-parametric model for the background; it approximates the probability density function of a background pixel distribution with a weighted average of a set of kernel functions defined around sample data points taken from the pixel location. The technique satisfies the requirements specified above and produces reasonable results. However, the resulting segmentations still contain some spurious results. Thus, we refined the algorithm by adding spatio-temporal continuity constraints to the background pixel distribution in the form of Markov random fields (MRF). The final background subtraction algorithm was tested using real data, and implemented to run in real time.

Data Collection

Since adequate video sensor data were not available from the SITEX experiments, the background subtraction algorithm was tested using data collected at Northwestern University. The data were collected for an outdoor scenario that consisted of vehicles moving on a road. Two USB cameras attached to laptop computers were used and the cameras were set to collect grayscale video at 15 frames per second at a resolution of 352x288 pixels. Included in the test cases were that of a single target moving at 20 mph, a single target starting at 10mph and increasing its speed to 20mph, a single target starting at 20mph, then stopping and idling for 1minute and then accelerating back to 20mph, and two targets moving in opposite directions at 20mph. The algorithm was shown to work well in windy, outdoor conditions, and was shown to be robust to changes in illumination caused by moving clouds.

Real-time Implementation

Once the algorithm was tested for accuracy, it was optimized for use in real-time applications. The algorithm was implemented in C using video4linux software, which is available on Linux iPAQs. It can run at 10 frames/sec on 320x240 pixel video data. The algorithm was implemented using only integer arithmetic in a manner that would make it simple to integrate the code with a handheld device such as an iPAQ.

Multiple Sensor Tracking and Sensor Selection

Due to their high-energy consumption, it is important to only keep a minimum number of sensors active in the network at any given time. Thus, we developed a method for selecting the optimal subset of imaging sensors to use for tracking a moving target such that the energy consumed in the network will be within a given constraint. The initialization time and energy required for initialization of the background subtraction algorithm was also considered as a factor in the sensor selection algorithm. The sensor data fusion for target tracking was performed using an unscented Kalman filter (UKF) formulation, which allows for non-linear dynamic and observation models and at the same time is simpler to implement and more accurate than an extended Kalman filter.

The proposed technique selects the best subset of sensors based on an optimization that maximizes the information utility of a set of active sensors over a finite time window

subject to a constraint on the energy consumption. The information utility of a subset of sensors is defined to be proportional to the entropy of the posterior distribution of the target state estimate given that only that subset of sensors is active. The method is based on the assumption that the target state distribution is unimodal and can be approximated by a Gaussian distribution. In the case of a Gaussian target state distribution, the covariance of the posterior distribution given measurements from a particular subset of sensors can be calculated prior to obtaining the actual measurements from the sensor subset.

This method was implemented in a simulated target-tracking scenario. In our simulations, the sensor field was divided into a grid of 10m x 10m blocks. Each block contained two imaging sensors that were arbitrarily placed and oriented within the block. We assumed that the sensors have been calibrated, and that they have a frame rate of 30fps. We also assumed that each block contains one processing node, which keeps track of the current target state and activates or deactivates the imaging sensors based on the sensor selection algorithm. It is assumed that the processing nodes can only communicate with imaging sensors that are within the neighboring blocks, and that only the processing node in the block that contains the target is active at any given time. As the target moves through the sensor field, the current processing node activates the optimal sensors, obtains measurements, and calculates the new target state statistics. When the target moves out of the block, the current processing node hands off the tracking task by activating the processing node in the neighboring block entered by the target. Our simulations were run for target speeds of up to 50mph, and comparisons were made between the proposed method for sensor selection and another random selection approach. The results clearly show the benefits of using the proposed method for optimal imaging sensor selection. Fig. 5 shows an example realization of the sensor network, and a target trajectory.

Low-transmission-energy techniques for communication of image and video data

We developed techniques that make efficient use of transmitter energy in video streaming over wireless channels. The goal was to efficiently utilize transmitter energy while meeting delay and video quality constraints. The key to the new techniques is the joint selection of coding parameters and transmitter power in order to minimize transmission energy for a given delay and video quality constraint.

Summaries of our results are presented in the publications [26] – [31].

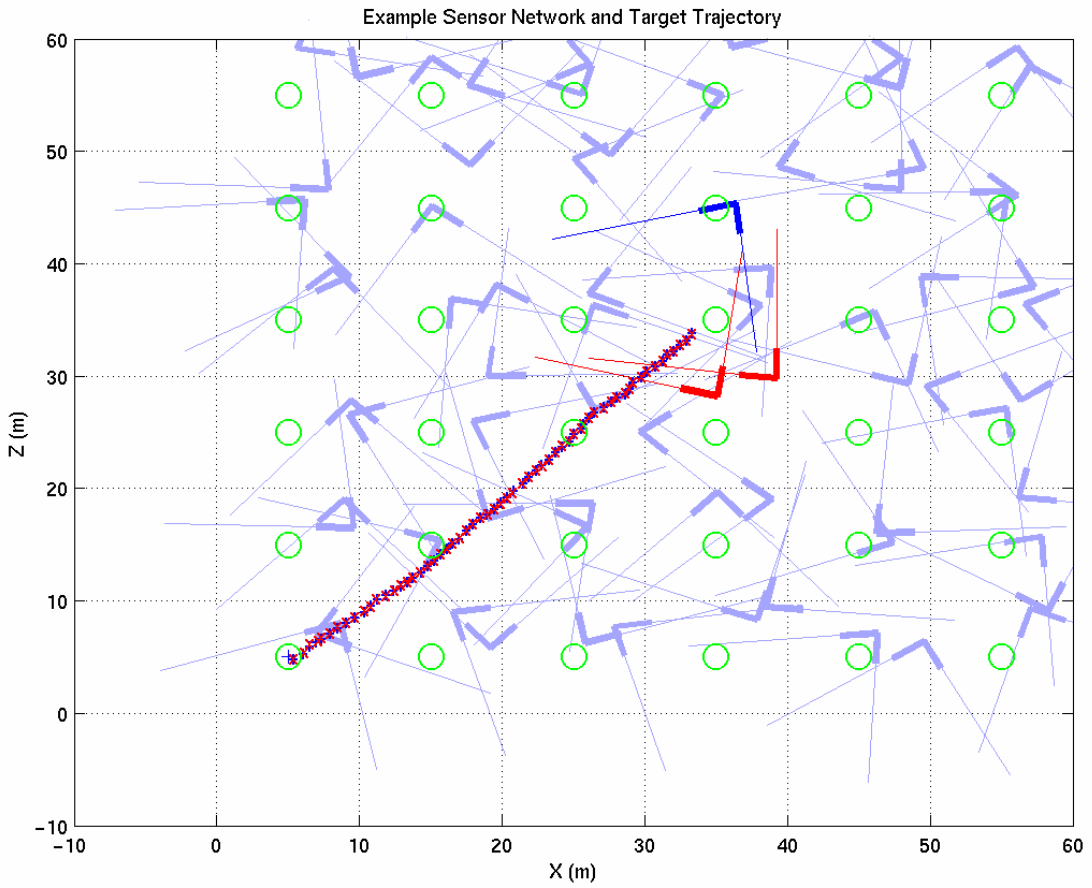

Figure 5 Sensor network showing fields of view of arbitrarily placed and oriented imaging sensors. The circles represent the positions of the processing nodes in each block. An example target trajectory through the network is also shown.

VI. Conclusions

The main goal of this project was to provide and compare the security /power tradeoffs of various cryptographic mechanisms for sensor networks. An added task on image processing via power conscious sensor network was also performed. Several new cryptographic techniques suited for low power applications have been developed, with attention to architectural and implementation issues. New imaging and tracking algorithms were also developed that further enables existing techniques. It is hoped that these could be integrated readily with current systems in a realistic application.

VII. References

[1] Muxiang Zhang, Christopher Carroll, Agnes H. Chan, “The Software-Oriented Stream Cipher SSC2”, Fast Software Encryption Workshop 2000

[2] Muxiang Zhang, Agnes H. Chan, “Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers”, CRYPTO 2000

[3] Philip Hawkes, Frank Quick and Gregory G. Rose, “A Practical Crypanalysis of SSC2”, Selected Areas in Cryptography 2001

[4] Duncan S. Wong, Hector Ho Fuentes, Agnes H. Chan, “The Performance Measurement of Cryptographic Primitives on Palm Devices”, The Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC 2001)

[5] H. P. Yuen, “KCQ: A new Approach to Quantum Cryptography”, Los Alamos preprint quant-ph 0311071.

[6] Chunhong Chen, Xioajian Yang, and Majid Sarrafzadeh, "Predicting Potential Performance for Digital Circuits," IEEE Transactions on CAD, Vol. 21, No. 3, March 2002, pp. 253-262.

[7] Ankur Srivastava, Eren Kursun, and M. Sarrafzadeh, “Predictability in RT-Level Designs”, Journal of Circuits, Systems and Computers, " special issue on Low Power IC Designs.

[8] Chunhong Chen, Elaheh Bozorgzadeh, Ankur Srivatsava, and Majid Sarrafzadeh, "Budget Management and Its Applications," to appear in Algorithmica.

[9] A. Srivastava E. Kursun and M. Sarrafzadeh, "Predictability in RTL-Designs", To Appear in Journal of Circuits, Systems and Computers (JCSC), Special Issue on Low Power IC Designs.

[10] Soheil Ghiassi, Ankur Srivastava, Xiaojian Yang, and Majid Sarrafzadeh ”Optimal Energy Aware Clustering in Sensor Networks”, Sensors 2002, 2, 258-269.

[11] A. Srivastava, J. Sobaje, M. Potkonjak and M. Sarrafzadeh, “, Optimal Node Scheduling for Effective Energy Usage in Sensor Networks,” A chapter in System-Level Power Optimization for Wireless Multimedia Communication, Kluwer Academic Publishers, 2002.

[12] Chunhong Chen and Majid Sarrafzadeh, "Simultaneous Volage Scaling and Gate Sizing for Low Power Design," IEEE Transactions on Circuits and Systems (Part II), June 2002 issue - vol. 49, no. 6, pp. 400-408.)

[13] R. Kastner, S. Ogrenci-Memik, E. Bozorgzadeh and M. Sarrafzadeh, "Instruction Generation for Hybrid Reconfigurable Systems", in International Conference on Computer-Aided Design (ICCAD), San Jose, CA, November, 2001.

[14] S. Ogrenci-Memik, E. Bozorgzadeh, R. Kastner, and M. Sarrafzadeh, “A Super-Scheduler for Embedded Reconfigurable Systems,” in International Conference on Computer-Aided Design(ICCAD), San Jose, CA, November 2001.

[15] Chunhong Chen and Majid Sarrafzadeh, "Power-Manageable Scheduling Technique for Control Dominated High-Level Synthesis", DATE 2002.

[16] Seda Ogrenci-Memik, Ankur Srivatsava, and Majid Sarradzadeh, “Design under Uncertainties”, International Symposium on Circuits & Systems, (ISCAS 2002); special session on COMPUTATIONAL GRAPH THEORY FOR COMPUTER AND COMMUNICATION SYSTEMS, Phoenix, AZ.

[17] Ankur Srivastava, J. Sobaje, Miodrag Potkonjak and Majid Sarrafzadeh, "Optimal Node Scheduling for Effective Energy Usage in Sensor Networks", IEEE Workshop on Integrated Management of Power Aware Communications, Computing and Networking 2002.

[18] Ankur Srivatsava and Majid Sarrafzadeh, "Predictability Driven Binding ", IEEE/ACM International Workshop on Logic & Synthesis (IWLS-02), New Orleans, Louisiana June 4-7, 2002.

[19] Eren Kursun, Ankur Srivastava, Seda Ogrenci Memik, Majid Sarrafzadeh, “Early Evaluation Techniques For Low Power Binding,” ISLPED'02: ACM/IEEE International Symposium on Low Power Electronics and Design.

[20] Chunhong Chen, Changjun Kang, and Majid Sarrafzadeh, “Activity-sensitive clock tree construction for low power,” A poster in ISLPED'02: ACM/IEEE International Symposium on Low Power Electronics and Design.

[21] Philip Brisk, Adam Kaplan, Ryan Kastner, and Majid sarrafzadeh, “Instruction Generation and Regularity Extraction For Reconfigurable Processors,” International Conference on Compilers, Architecture and Synthesis for Embedded Systems, CASES 2002 (Grenoble, France, October 8-11, 2002.

[22] E. Bozorgzadeh, S. Ghiasi, A. Takahashi, and M. Sarrafzadeh, "Optimal Integer Delay Budgeting on Directed Acyclic Graphs", DAC 2003, Anaheim.

[23] A. Srivastava and M. Sarafzadeh, "Predictability: Definition Analysis and Optimization", International Conference on Computer Aided Design, 2002.

[24] A. Srivastava, S. Ogrenci Memik, B.K. Choi and M. Sarrafzadeh:,"Achieving Design Closure Through Delay Relaxation Parameter", International Conference on Computer Aided Design 2003.

[25] A. Srivastava, R. Kastner, C. Chen and M. Sarrafzadeh, "Timing Driven Gate Duplication", To Appear in IEEE Trans on VLSI Systems P. V.

[26] Pahalawatta, D. Depalov, T.N. Pappas, and A.K. Katsaggelos, “Detection, Classification, and Collaborative Tracking of Multiple Targets Using Video Sensors.” Int. Workshop on Information Proc. Sensor Networks (IPSN), pp. 529-544, April 22-23, 2003.

[27] Y. Eisenberg, F. Zhai, C.E. Luna, T.N. Pappas, R. Berry, and A.K. Katsaggelos, “Variance-Aware Distortion Estimation and Reduction for Wireless Video Communications,” Proc. Int. Conf. Image Processing, vol. 1, (Barcelona, Spain), pp. 89-92, Sept. 2003

[28] Y. Eisenberg, C. Luna, T. N. Pappas, R. Berry, and A. K. Katsaggelos, "Joint Source Coding and Transmission Power Management for Energy Efficient Wireless Video Communications," Special Issue on Wireless Video, IEEE Trans. Circuits and Systems for Video Technology, vol. 12, no. 6, pp. 411-424, June 2002.

[29] C.E. Luna, Y. Eisenberg, R. Berry, T.N. Pappas, and A.K. Katsaggelos, “Joint Source Coding and Data Rate Adaptation for Energy Efficient Wireless Video Streaming,” IEEE Journal on Selected Areas in Communications, Special Issue on “Recent Advances in Wireless Multimedia,” vol. 21, no. 10, pp. 1710-1720, Dec. 2003.

[30] F. Zhai, C.E. Luna, Y. Eisenberg, T.N. Pappas, R. Berry, and A.K. Katsaggelos, “Joint Source Coding and Packet Classification for Video Streaming Over Differentiated Services Networks,” IEEE Transactions on Multimedia, Special Issue on “Streaming Video.” To appear.

[31] J. Chen, T.N. Pappas, A. Mojsilovic, B. Rogowitz, “Perceptual color and texture features for segmentation,” in Human Vision and Electronic Imaging VIII, Proc. SPIE vol. 5007, (Santa Clara, CA), pp. 340-351, Jan. 2003.